

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

JANE DOE,

Plaintiff,

v.

COUNTY OF SANTA CLARA,

Defendant.

Case No. [23-cv-04411-WHO](#)

**ORDER ON MOTION TO DISMISS**

Re: Dkt. No. 47

Plaintiff brings this class action on behalf of all patients or prospective patients of the Santa Clara Valley Medical Center (“SCVMC”) who exchanged communications with SCVMC through SCVMC’s websites and patient portal. Second Amended Complaint (“SAC”) ¶ 334. Defendant County of Santa Clara moves to dismiss each of the claims asserted against it. For the reasons discussed below, that motion is GRANTED in part and DENIED in part.

**BACKGROUND**

Plaintiff is a resident of Santa Clara County, California, who alleges that she has used SCVMC’s website and patient portal (“Portal”) since 2018 to search for doctors, access her lab results, schedule doctor’s appointments, refill prescriptions, and communicate with her doctors.<sup>1</sup> SAC ¶ 18. She states that during “her interactions inside the patient portal” she entered sensitive medical information relating to her endometriosis, pelvic floor disorder, and menopause issues into the patient portal. *Id.* ¶ 21. She contends that she has used Santa Clara’s website to order medications for women’s health issues, including endometriosis, as well as for pancreatitis, asthma, fibromyalgia, and pain management. *Id.* ¶¶ 21, 24 (collectively, “Personal Health

---

<sup>1</sup> Defendant is defined as the County of Santa Clara d/b/a Santa Clara Valley Medical Center. Defendant is the County and while the County moves to dismiss SCVMC as a defendant, Mot. at 12, plaintiff clarified that SCVMC is not a separately named defendants, but just the d/b/a of the County. *Oppo.* at 1 n.1.

Information” or “PHI”). On information and belief, she asserts that defendant installed “tracking pixels” on its website and patient portal that surreptitiously forward patient interactions including her healthcare information and information that could be used to personally identify her to third parties, including Meta/Facebook and Google. *See, e.g., id.* ¶¶ 21, 22, 27.

Plaintiff sues on behalf of two classes: the “Santa Clara Valley Medical Center Class: For the period August 25, 2018, to the present, all patients or prospective patients of Santa Clara Valley Medical Center or any of its affiliates who exchanged communications at Santa Clara Valley Medical Center’s websites” and “The Patient Subclass: For the period August 25, 2018, to the present all patients of Santa Clara Valley Medical Center or any of its affiliates and who exchanged communications at Santa Clara Valley Medical Center’s websites.” *Id.* ¶ 334. She asserts the following causes of action: (1) Violation of the California Invasion of Privacy Act (“CIPA”) Cal. Penal Code §§ 630, *et seq.* (2) Violation of (“CMIA”) Cal. Civil Code § 56.101; (3) Violation of CMIA, Civil Code § 56.10; (4) Violation of the Comprehensive Computer Data Access and Fraud Act (“CDAFA”) Cal. Penal Code § 502; (5) Violation of Cal. Civil Code § 1798.82; (6) Common Law Invasion of Privacy Intrusion Upon Seclusion; and (7) Violation of the Information Practices Act (“IPA”) Cal. Civil Code § 1798.1, *et seq.*

The County moves to dismiss each claim.<sup>2</sup>

### LEGAL STANDARD

Under FRCP 12(b)(6), a district court must dismiss a complaint if it fails to state a claim upon which relief can be granted. To survive a Rule 12(b)(6) motion to dismiss, the plaintiff must allege “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible when the plaintiff pleads facts that “allow the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted). There must be “more than a sheer possibility that a defendant has acted unlawfully.” *Id.* While courts do not require “heightened fact pleading of specifics,” a plaintiff must allege facts sufficient to “raise a

---

<sup>2</sup> Plaintiff does not oppose the County’s motion to dismiss the IPA claim, *Oppo*. at 20, and the County’s motion to dismiss the IPA claim is GRANTED.

right to relief above the speculative level.” *Twombly*, 550 U.S. at 555, 570.

In deciding whether the plaintiff has stated a claim upon which relief can be granted, the Court accepts the plaintiff’s allegations as true and draws all reasonable inferences in favor of the plaintiff. *See Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987). However, the court is not required to accept as true “allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences.” *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008). If the court dismisses the complaint, it “should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts.” *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000). In making this determination, the court should consider factors such as “the presence or absence of undue delay, bad faith, dilatory motive, repeated failure to cure deficiencies by previous amendments, undue prejudice to the opposing party and futility of the proposed amendment.” *Moore v. Kayport Package Express*, 885 F.2d 531, 538 (9th Cir. 1989).

## DISCUSSION

### I. CONTRACT DEFENSES – CONSENT AND WAIVER

The County argues that plaintiff’s claims are barred by consent and/or waiver by her agreement to two enforceable contracts: the County’s judicially noticeable “website privacy policy” (“Website Privacy Policy”) which is available on the County’s website, and the “Terms and Conditions” (“T&Cs”) users agree to in order to access the SCVMC’s patient Portal. Plaintiff disputes the meaning and intent of the disclosures contained in the Website Privacy Policy and the T&Cs. She instead points to the County’s Notice of Privacy Practices to support her alleged breach of contract and privacy claims.

#### A. Website Privacy Policy, Portal T&C, Notice of Privacy Practices

The County relies on the following disclosures in Website Privacy Policy, which it claims bars plaintiff’s breach of contract and privacy claims as a matter of law:

#### 2. INFORMATION WE COLLECT AND YOU SHARE

##### 2.1 Information We Collect

##### Key Points:

**We automatically collect several categories of information, including IP address, date and time of visit, and which pages you visit on our site.**

Analytics companies may use this information as well, typically in aggregate, to determine, for example, which web pages get the most or least traffic.

When you access this website, we automatically collect several categories of information, including the following:

- ☐ Your Internet Protocol (IP) address (a unique set of numbers and/or letters that generally identifies the network from which devices access the internet)
- ☐ The referring address, if any (this would tell us the address of the website you used to get to sccgov.org, such as through a Google search or link)
- ☐ The size and resolution of your monitor and the size of the browser window
- ☐ The type of browser (e.g., Firefox, Edge, Chrome) used to access our site
- ☐ The operating system (e.g., Windows, Mac OS, Unix) used to access our site
- ☐ The city in which your IP address originates
- ☐ The date and time of your visit, and the total time you spend on the site
- ☐ The time you spend on each page and in what order those pages were visited
- ☐ The internal links you click

We provide this information to analytics companies including Siteimprove and Google Analytics. They typically aggregate the information and present it in a format that allows us to quickly determine how many people are visiting the site, which pages are most popular, and other similar information.

RJN, Ex. E (Website Privacy Policy, as of Nov. 2019) at 2.

The Website Privacy Policy also discloses:

### **2.1.1 User Tracking**

#### **Key Points:**

We do use website tracking technologies, such as cookies and pixels, to track visitors to the website. Other third-party services on our site may do so as well.

We obtain some of the information described in Section 2.1 by using website tracking technologies to track your visit, which may include cookies, pixels, tags, beacons, and similar technologies. These technologies allow us to provide website functionality and understand how you interact with the sccgov.org website.

We also embed some content on our site using third-party web widgets and services such as Facebook, Twitter, YouTube, Instagram,

and Flickr. These third parties may set their own cookies and similar technologies for functional and tracking purposes. They may have their own privacy, security, terms of service, and accessibility policies applicable to the features they provide. For more information about third-party services and their policies, please visit their websites.

### 2.1.2 Why We Collect This Information

#### Key Points:

We typically use this information to help understand how users interact with the website, to maintain its functionality, and improve the user experience.

We automatically collect this information typically in order to understand how users interact with our website and promote its functionality. For example, cookies and similar technologies can tell us the number of visitors the website receives, whether and how often individuals return, and what they look for when they arrive. This helps us understand what people are looking for, which web pages are most useful, and other similar information that we can use to improve the experience of visiting sccgov.org. Cookies also help us maintain communication between visitors' computers and County servers.

*Id.* at 3. The December 2021 version is materially similar.<sup>3</sup>

The County also relies on disclosures from the T&Cs that it contends users of the Patient Portal had notice of when using the Portal. The County asserts that the T&C were linked on the bottom of the Portal landing page. *See* Request for Judicial Notice, Exs. G (current T&C) & H (T&C from 2020). It points to the following disclosures in the T&C:

[The County] is pleased to offer our patients online computer access to portions of their medical record and related services through this site while you are admitted at our facility. This access is subject to your completion of an authorization and compliance with the terms, conditions, and notices set forth below. SCVH reserves the right to limit or terminate your use of myHealth Online if you fail to abide by the Terms and Conditions. Please take the time to review them carefully.

...

Acceptance of Terms and Conditions

*When you access, use or view this website ('myHealth Online'), you thereby agree to be bound by this agreement regarding the terms and*

<sup>3</sup> The County also relies on the policy in place from June 2016 through November 2019, arguing that it informs users of the SCVMC website of “what personal information about visitors is collected on this site” and “under what conditions this information may be shared or released to another party.” RJN, Ex. D (June 2016 version) at 1; *see also id.* at 3 (disclosing the use of “persistent” cookies on County website, including that they “can contain data about user movement during the visit to the website”). That policy also informs users of the SCVMC website that “the County does not guarantee the absolute security of information it maintains.” *Id.* at 4.

conditions of use (“Terms and Conditions”). Please note that SCVH may revise these Terms and Conditions at any time by updating this posting. If you access, use or view this website after such revisions have been made, you may be required to accept the revised Terms and Conditions and you will be bound by them; therefore, we advise you to periodically review this page for such revisions. If you do not agree to these Terms and Conditions, please exit this website promptly.

RJN Exs. G (emphasis added). The T&C also disclose:

Upon accessing myHealth Online or the internet using the county-provided iPad, our web server collects and stores the following information: (1) the domain name from which you access the Internet; (2) the date and time you access the site; (3) the pages you visit; (4) the address of the website from which you linked directly to us; (5) the name and release number of the web browser software you are using; and (6) the IP (Internet Protocol) address of the computer you are using. This information may be used by SCVH for internal evaluation, quality control, and other reasons deemed appropriate by SCVH.

*Id.*

The County also relies on the following language from the T&C:

#### Security; Risks of Using Secure Sites and Secure Messaging

SCVH uses SSL encryption technology and takes other precautions to ensure that the information contained or transmitted via HTTPS is as secure as reasonably possible from unauthorized use or access. SCVH is using industry-standard encryption technologies to protect and secure the myHealth Online site, including the secure messaging function. Because of the added security of web-based, encrypted messaging, SCVH strongly recommends the use of secure messaging via myHealth Online, instead of e-mail, for online communications.

However, please note that while SCVH takes measures to safeguard your security, we cannot guarantee absolute security of the system against inadvertent disclosure or intentional intrusion. The use of electronic communication systems such as the World Wide Web (including secure messaging) for communications has several risks that users should consider before use. Such risks include, but are not limited to, the following: Electronic communications can be copied, circulated, forwarded and stored, in numerous paper and electronic files. Electronic communications can be accidentally broadcast worldwide and received by many unintended recipients. Backup copies of electronic communications may exist even after the originator or recipient has deleted his or her own copy. Employers and online services have a right to archive and inspect e-mails transmitted through their systems. Message senders can misaddress a message. Messages can be intercepted, altered, forwarded, or used without written permission or detection. E-mail notifications can be used to introduce viruses into computer systems. Electronic communications are discoverable and may be used as evidence in court. Passwords providing access to electronic communications can be stolen and misused, or host systems can be compromised, leading



to unauthorized disclosures of personal information.

Because of these risks, SCVH cannot guarantee the security and confidentiality of secure messaging and other communication submitted through myHealth Online and will not be liable for improper disclosure of confidential information. *YOU HEREBY EXPRESSLY ASSUME THE SOLE RISK OF ANY INTENTIONAL INTRUSION, UNAUTHORIZED DISCLOSURE, FAILURE, DELAY, INTERRUPTION OR CORRUPTION OF DATA OR OTHER INFORMATION TRANSMITTED IN CONNECTION WITH THE USE OF THIS SERVICE.*

*Id.* (italization added).

#### Warranties and Disclosures

You assume risk for all use of this website. FURTHER, THIS WEBSITE IS PROVIDED BY SCVH ON AN "AS IS" AND "AS AVAILABLE" BASIS; AS SUCH SCVH ASSUMES NO LIABILITY OR RESPONSIBILITY FOR ANY ERRORS OR OMISSIONS IN, OR RELIANCE UPON, THE INFORMATION ON THIS SITE. SCVH MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO: ACCURACY, COMPLETENESS, OR AVAILABILITY OF CONTENT, NON-AGENTS AND ASSIGNS ARE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS OR THAT THE MYHEALTH ONLINE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS WILL BE CORRECTED. INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE OR PURPOSE, TO THE FULLEST EXTENT OF THE LAW. SCVH DOES NOT WARRANT THAT THIS WEBSITE, ITS SERVERS, OR E-MAIL SENT FROM THE SITE OR ITS DIRECTORS, OFFICERS, or EMPLOYEES.

#### Limitations of Liability; Indemnity

TO THE MAXIMUM EXTENT PERMITTED BY LAW, SCVH AND ITS DIRECTORS, OFFICERS, EMPLOYEES, AGENTS AND ASSIGNS SHALL NOT BE LIABLE TO YOU OR ANYONE ELSE FOR ANY DAMAGES OR INJURY, INCLUDING, BUT NOT LIMITED TO, DIRECT, INDIRECT, CONSEQUENTIAL, SPECIAL, INCIDENTAL, PUNITIVE DAMAGES, PERSONAL INJURY, MENTAL ANGUISH, EMOTIONAL DISTRESS, OR WRONGFUL DEATH THAT RESULT FROM THE USE OF, OR INABILITY TO USE THIS SITE OR THE MATERIALS PROVIDED ON THIS SITE, OR THE SERVICES OR PRODUCTS RECEIVED FROM THIS SITE.

THIS INCLUDES, BUT IS NOT LIMITED TO, DAMAGES RESULTING FROM ACTIONS TAKEN BY YOU OR OTHERS IN RELIANCE ON INFORMATION CONTAINED IN THIS SITE, MISDIRECTION OR INTERCEPTION OF INFORMATION, INTENTIONAL OR UNINTENTIONAL BREACHES AND ACCESS BY THOSE YOU PROVIDE YOUR USERNAME AND PASSWORD TO. YOU AGREE THAT SCVH SHALL NOT BE LIABLE FOR ANY DAMAGES UNDER ANY

INDEMNITY OR ANY THEORY, INCLUDING, WITHOUT LIMITATION, LIABILITY ARISING OUT OF CONTRACT, NEGLIGENCE, STRICT LIABILITY, TORT, PATENT OR COPYRIGHT INFRINGEMENT. SCVH TAKES NO RESPONSIBILITY FOR, AND DISCLAIMS ANY AND ALL LIABILITY ARISING FROM, ANY INACCURACIES OR DEFECTS IN SOFTWARE, COMMUNICATION LINES, VIRTUAL PRIVATE NETWORK, THE INTERNET OR YOUR INTERNET SERVICE PROVIDER (ISP), ACCESS SYSTEM, COMPUTER HARDWARE OR SOFTWARE, OR ANY OTHER SERVICE OR DEVICE THAT YOU USE TO ACCESS MYHEALTH ONLINE.

In consideration for SCVH's permitting you to use myHealth Online you expressly release and hold harmless SCVH, its officers, directors, employees, agents, and assigns from any and all claims, liabilities, demands, causes of action, costs, expenses, and damages of every kind and nature, in law or equity, or otherwise, arising out of or in any way related to your use of myHealth Online, whether arising from negligence or any other acts or omissions by SCVH. In addition, you will indemnify and hold harmless SCVH, its officers, directors, agents, affiliates, and employees, against all actual and direct losses, liabilities, damages, claims, costs or expenses (including reasonable attorney's fees) they may suffer as the result of third party claims, demands, actions, investigations, settlements or judgments against them arising from or in connection with any breach of these Terms and Conditions, or from any breaches of confidentiality or negligence or wrongful acts or omissions, by you or your dependents, or agents. The provisions of this section entitled "Limitations of Liability; Indemnity" shall survive termination of this agreement.

*Id.*

Finally, the County notes that as of some unspecified date, in order to set up a Portal account, users are or were required to affirmatively select "Accept" or "Decline" noting their acceptance of the hyperlinked T&C. RJN, Ex. K.

Plaintiff does not oppose defendant's Request for Judicial Notice of these documents, and the request to notice Exhibits D-K is GRANTED.<sup>4</sup> Plaintiff, in addition, requests judicial notice

---

<sup>4</sup> Plaintiff does object to defendant's request that I take judicial notice of the legal arguments asserted in litigation by the American Hospital Association ("AHA") and other non-parties. *See* RJN, Exs. A-C. I agree and DENY the request to take judicial notice of AHA's motion for summary judgment, an amici brief submitted by 30 hospitals, and the amici brief of state hospital associations. The County seeks judicial notice of those litigation documents for the fact that "courts are being asked to adjudicate the constitutionality and legality of the new rules issued by the U.S. Department of Health and Human Services (HHS) that prohibit the use of certain tracking technologies that make healthcare providers' webpages more effective." *See* Mot. at 1 n.1. The ongoing challenges to the HHS rules are irrelevant to whether plaintiff has stated her claims in this case; the HHS rules are currently in effect and are only one group of facts that support the plausibility to plaintiff's statutory and common law claims.



of the County’s Notice of Privacy Policy, which I also GRANT. *See* Dkt. No. 54-1, Ex. A (“Notice”). The Notice of Privacy Policy governs how the County of Santa Clara Health System may use and disclose “medical information about you.” The Notice provides:

**Marketing and Sale of PHI**

We may not use or disclose your PHI for marketing purposes without your written authorization. We may not sell your PHI without your written authorization.

*Id.* at 6.

**B. Consent to Tracking**

The County contends that by referencing the County’s Website Privacy Policy in her SAC, plaintiff had actual or constructive notice of its disclosures. It argues that those disclosures put a reasonable person on notice that “tracking technologies” including cookies and pixels placed by third parties would collect both personally identifiable information regarding plaintiff’s use of the County’s website, including the PHI at issue. That consent, according to the County, undermines each of plaintiff’s claims. The County also points to disclosures that third parties like “Facebook, Twitter, YouTube, Instagram” and others may have embedded “their own” cookies for “functional and tracking purposes” and encouraged website users to visit those third-party sites for more information about their tracking or block the use of cookies.

That plaintiff included reference to the Website Privacy Policy in her SAC – to support the plausibility of her allegations – does not mean that she personally knew of those policies as of a particular time (*e.g.*, before having retained counsel) sufficient to demonstrate consent to those policies and bar her claims. If and when she learned of the Website Privacy Policy is not irrelevant, but that may be explored in discovery.

More significantly, taking plaintiff’s allegations as true, the disclosures identified by the County do not foreclose her claims based on the disclosure of her healthcare-related data. Those disclosures may, read favorably to the County, indicate that some personally identifiable information might be disclosed “typically” in aggregated form for defendant’s purposes. But nothing in the provisions identified by the County disclose the disclosure of PII, much less PHI, to third parties for those third parties’ own use. *See Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d

1 1064, 1078 (N.D. Cal. 2023) (quoting *Brown v. Google LLC*, No. 4:20-CV-3664-YGR, 685  
2 F.Supp.3d 909, 926 (N.D. Cal. Aug. 7, 2023) (“For consent to be actual, the disclosures must  
3 ‘explicitly notify’ users of the practice at issue.”)).

#### 4 **C. Waiver of Liability**

5 The County next argues that by agreeing to the T&C before using the Portal, plaintiff has  
6 agreed to the limitations of liability clause and cannot sue the County for disclosing her PHI  
7 connected to her use of the Portal. In support, it seeks Judicial Notice of Exhibit K – a screen shot  
8 of the current sign-up process requiring users to affirmative accept or decline the T&C to create a  
9 portal account. It provides *no information* of the date that page became active or when affirmative  
10 consent was otherwise required.

11 Plaintiff pleads that she has been using the Portal since 2018. SAC ¶ 18. Therefore, the  
12 contents of the current account creation page is irrelevant. Similarly, the County’s reliance on the  
13 current and January 2022 archived “myHealth Online Patient Quick Start Guides” do not establish  
14 that affirmative consent was required when plaintiff started using the Portal in 2018. Consent to  
15 T&C has not been established because the County has not shown that *when plaintiff* created her  
16 account she was required to affirmatively consent to the T&C. *See* RJN, Exs. I-K.

17 Separately, the County argues that plaintiff agreed to the T&C as a browsewrap agreement,  
18 because the T&C are hot linked at the bottom of at least the landing page for the Portal. *See* SAC  
19 ¶ 32 (showing current hyperlinked T&C at bottom of Portal sign-in page). But again, it has failed  
20 to meet its burden to show that plaintiff had to take some affirmative act demonstrating assent to  
21 the T&C by her continued use of the Portal, nor has the County addressed the numerous cases  
22 within the Ninth Circuit that have addressed how a browsewrap agreement must be presented to a  
23 continuing user of a website in order to support constructive assent. Absent that effort and  
24 showing, I will not find that plaintiff’s claims are barred by the substantive disclosures or  
25 limitation of liability provisions in the T&C.<sup>5</sup>

---

26  
27 <sup>5</sup> The County’s argument that simply because the T&C are referenced in her SAC, plaintiff has  
28 shown affirmative assent making them binding on plaintiff, is wholly unsupported by any  
statutory or caselaw support. Plaintiff, in a declaration submitted with the Opposition, makes clear  
that she did not have actual notice of the Website Privacy Policy or T&C prior to disclosing her

The County's motion to dismiss based on consent and waiver is DENIED.

## II. CIPA

The County moves to dismiss plaintiff's CIPA claim because a public entity is not a "person" who may be a defendant on CIPA claim. *See Doe v. Regents of Univ. of California*, 672 F. Supp. 3d 813, 817–18 (N.D. Cal. 2023 ("Because the text of CIPA does not expressly include liability for public entities, I find that UC Regents is immune from liability under CIPA.")).

Plaintiff does not oppose dismissal. Instead, she seeks leave to allege a Federal Wiretap Act claim under 18 U.S.C. section 2520(a) in place of her CIPA claim. The County opposes the request for leave to amend, arguing that she offers no explanation why she did not allege this claim earlier nor what facts she would offer in support of it, and that in any event leave to amend should be denied because it would be futile because a section 2520 claim does not apply to public entities.

Both sides note that there is a split in caselaw regarding whether a section 2520 claim can be applied to a public entity. *Compare Seitz v. City of Elgin*, 719 F.3d 654, 657 (7th Cir. 2013) (government entities may not be sued under Section 2520, but cases holding the contrary); *Head v. Cnty. of Sacramento*, No. 219CV01663TLNCKD, 2020 WL 3429485, at \*3 (E.D. Cal. June 23, 2020 ("This court finds the Seventh Circuit's analysis persuasive and follows the Central District Court of California in adopting *Seitz*'s holding. *See Federated Univ. Police Officers' Ass'n v. Regents of Univ. of California*, No. SACV 15-00137-JLS-, 2015 WL 13273308, at \*8 (C.D. Cal. July 29, 2015)); *with Adams v. City of Battle Creek*, 250 F.3d 980 (6th Cir. 2001) (governmental entities may be held liable for violations of Wiretap Act); *Medina v. Cnty. of Riverside*, No. CV 06-4144 ABC (EX), 2006 WL 8437749, at \*4 (C.D. Cal. Dec. 1, 2006) ("The federal wiretap

---

PHI through the website or Portal. Dkt. No. 54-4, ¶¶ 2-4. The County moves to strike that declaration because it attempts to introduce matters "outside the scope of the SAC." Dkt. No. 58 at 3. The motion to strike is DENIED. Absent apposite authority binding plaintiff to the T&C simply because they were cited in her SAC – as opposed to showing actual or constructive assent based on how and when the T&C were presented to plaintiff – I reject defendant's argument; I do not reach whether if sufficient assent had been demonstrated by the County, the T&C would bar plaintiff's claims. Nor do I reach plaintiff's position that any bar would be void under Cal. Civ. Code § 1668. *Oppo.* at 12. These arguments may be reraised after discovery on summary judgment or otherwise.

statutes are applicable to counties and other governmental entities.”).

Plaintiff is given leave to amend to add a section 2250(a) claim. If the County believes that the weight of authority in the Ninth Circuit would preclude it, the County may move to dismiss it from the further amended complaint, allowing for a more expansive discussion of the split in caselaw.

The County’s motion to dismiss the CIPA claim is GRANTED with prejudice, but plaintiff is given leave to allege a claim under the Federal Wiretap Act.

### III. CDAFA

The County argues that it cannot be a defendant for the claimed violation of the Comprehensive Computer Data Access and Fraud Act (“CDAFA,” Cal. Penal Code § 502) because the County is not a “person” within the meaning of the Act. The County relies on my decision in *Doe v. Regents of Univ. of California*, 672 F. Supp. 3d 813, 817–18 (N.D. Cal. 2023). There, following *Wells v. One2One Learning Foundation*, 39 Cal. 4th 1164, 1192 (2006), I found that the Regents of the University of California were exempt as a public entity from the scope of the California Invasion of Privacy Act (“CIPA,” Cal. Pen Code § 631). Neither side cites cases discussing CDAFA specifically (as opposed to CIPA). However, I need not resolve this issue because plaintiff’s CDAFA claim fails for a different reason.

Even if the County is a person that can be sued under CDAFA, plaintiff has failed to allege the requisite loss or damage required under the statute. CDAFA provides that only an individual who has “suffer[ed] damage or loss by reason of a violation” of the statute may bring a civil action “for compensatory damages and injunctive relief or other equitable relief.” Cal. Penal Code § 502(e)(1). CDAFA permits recovery of “[c]ompensatory damages [that] include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access.” *Id.*

The damages under CDAFA alleged by plaintiff are:

- (a) Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;
- (b) Defendants eroded the essential confidential nature of the doctor-

patient relationship;

(c) Defendants took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

(d) Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Santa Clara's duty to maintain confidentiality; and

(e) Defendants' actions diminished the value of Plaintiff and Class Members' personal information.

SAC ¶ 395. In Opposition, plaintiff argues that these damages – based on the value of the data that the County took and derived a benefit from given the multi-billion-dollar industry for the sale and purchase of private medical data – suffices. Dkt. No. 54 at 15.

This argument fails. In *Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461 (N.D. Cal. 2021), the Hon. Donna M. Ryu rejected a theory of loss or damage under CDAFA based on the “loss of the right to control their own data, the loss of the value of their data, and the loss of the right to protection of the data.” *Id.* at 488. That type of loss was not covered by the statute and plaintiffs, therefore, lacked standing for their CDAFA claim. *See id.* (relying on *Nowak v. Xapo, Inc.*, No. 5:20-cv-03643-BLF, 2020 WL 6822888, at \*4-5 (N.D. Cal. Nov. 20, 2020) (dismissing CDAFA claim based on loss of value of stolen cryptocurrency in part because the nature of the loss was not cognizable under CDAFA)).<sup>6</sup> In *Doe v. Meta Platforms, Inc.*, No. 22-CV-03580-WHO, 2023 WL 5837443 (N.D. Cal. Sept. 7, 2023), I followed *Cottle* and dismissed the CDAFA claim based on damage as the lost value in plaintiff's PHI. *Id.* \*9.<sup>7</sup> The same result follows here.

The County's motion to dismiss the CDAFA claim is GRANTED. If plaintiffs have a viable theory of damages not based on the value of the PHI, they are given leave to amend.

---

<sup>6</sup> Plaintiff relies on my opinion in *In re Meta Healthcare Pixel Litig.*, No. 22-CV-03580-WHO, 2024 WL 333883 (N.D. Cal. Jan. 29, 2024). But there, CDAFA loss or damage was adequately alleged based on “revised allegations identifying the measurable impact on their devices,” and not on a theory that the value of PHI was diminished or Meta was unjustly enriched by use of that PHI. *Id.* at \*3. In my prior decision in that case, I followed *Cottle* and dismissed the CDAFA damage theory based on the “diminished value of information.” *Doe v. Meta Platforms, Inc.*, No. 22-CV-03580-WHO, 2023 WL 5837443, at \*9 (N.D. Cal. Sept. 7, 2023).

<sup>7</sup> Plaintiff also relies on *Brown v. Google LLC*, No. 4:20-CV-3664-YGR, 2023 WL 5029899, at \*19 (N.D. Cal. Aug. 7, 2023). But the issue there was general browsing history, not PHI. In PHI cases like this one – where plaintiffs allege that their privacy has been invaded because of the disclosure of sensitive and private healthcare information – plaintiffs cannot base their CDAFA damages on a theory that they lost a benefit to sell that data themselves.

#### IV. CCRA

The County moves to dismiss plaintiffs' claim under California Civil Code section 1798.82, the California Consumers Records Act ("CCRA"), arguing that as for the CDAFA, the County is not a proper defendant because it is not a person or a business.<sup>8</sup> Neither side relies on caselaw other than my decision in *Doe v. Regents of Univ. of California*, 672 F. Supp. 3d at 817–18, and the California Supreme Court decision in *Wells v. One2One Learning Foundation*, 39 Cal. 4th at 1192. Both cases addressed different statutes. And while plaintiff invoked the concept of legislative history of the CCRA, neither plaintiff nor the County cite particular provisions of the legislative history.

I will not determine this issue of state law on this record. If plaintiff further amends her complaint (in response to this Order), the County may move again to dismiss this claim. Or defendant may raise this issue on summary judgment. If and when the issue is joined in the future, the parties shall cite statutory and caselaw to support their respective positions. At this juncture, however, the motion to dismiss the CCRA claim is DENIED without prejudice.

#### V. COMMON LAW INVASION OF PRIVACY

Finally, the County moves to dismiss the invasion of privacy claim, arguing that it cannot be liable for a common law tort under California's Government Code. *See* Cal. Govt. Code § 815 ("Except as otherwise provided by statute: (a) A public entity is not liable for an injury, whether such injury arises out of an act or omission of the public entity or a public employee or any other

---

<sup>8</sup> Cal. Civ. Code § 1798.82. "Person or business who owns or licenses computerized data including personal information; breach of security of the system; disclosure requirements  
 (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."



person”); *see also Ruskell v. N. Cnty. Fire Prot. Dist. of Monterey Cnty.*, No. 15-CV-03540-BLF, 2016 WL 1365949, at \*2 (N.D. Cal. Apr. 6, 2016) (dismissing common law invasion of privacy claim against County).

Plaintiff argues that a subsequent but related section of the California Government Code, section 815.6, provides an exception: “Where a public entity is under a mandatory duty imposed by an enactment that is designed to protect against the risk of a particular kind of injury, the public entity is liable for an injury of that kind proximately caused by its failure to discharge the duty unless the public entity establishes that it exercised reasonable diligence to discharge the duty.” Plaintiff argues that this code provision would apply and allow tort liability against the County given its duties under both federal law (citing the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and 45 C.F.R. § 164.508) and state law (citing the Confidentiality of Medical Information Act (“CMIA,” Cal. Civ. Code § 56.10)). *See* Dk.t No. 54 at 16-20. However, plaintiff’s complaint does not assert a cause of action under Government Code section 815.6 or identify what mandatory duty the County may have violated.

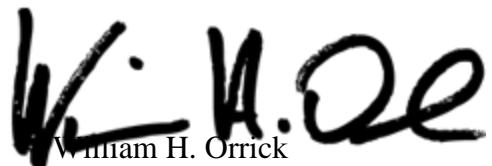
The County’s motion to dismiss the invasion of privacy claim under section 815 is GRANTED. Plaintiff is given leave to amend to state a claim under section 815.6 if she is able to identify a mandatory duty. The County’s arguments that neither the CMIA nor HIPAA can provide a basis for the duty will be addressed if plaintiff includes this claim in her further amended complaint and bases that claim on those statutory duties.

### CONCLUSION

The motion to dismiss is DENIED on the consent and waiver defenses and on the CCRA claim. The motion is GRANTED on the CIPA claim, the CDAFA claim, and the privacy claims. Plaintiff is given leave to amend her CDAFA and privacy claims and is given leave to state a Federal Wiretap Act claim. Any further amended complaint shall be filed within twenty-one (21) days of the filing of this Order.

**IT IS SO ORDERED.**

Dated: July 8, 2024

  
William H. Orrick  
United States District Judge